Projet de consultation publique
Exigence thématique Résilience organisationnelle

Le Cadre de référence international des pratiques professionnelles® de l'IIA comprend les Normes internationales d'audit interne™, les Exigences thématiques et les Lignes directrices internationales. Les Exigences thématiques sont obligatoires et doivent être utilisées conjointement avec les Normes, qui font autorité pour les pratiques requises.

Les Exigences thématiques définissent des attentes claires pour les auditeurs internes en fixant une référence minimale pour l'audit des domaines présentant des risques spécifiques. Le profil de risque de l'organisation peut rendre nécessaire que les auditeurs internes tiennent compte des dimensions supplémentaires de ce thème.

La conformité aux Exigences thématiques renforcera la cohérence des activités d'audit interne et améliorera leur qualité et leur fiabilité ainsi que leurs résultats. En fin de compte, les Exigences thématiques élèvent le niveau de la profession d'audit interne.

Les auditeurs internes doivent appliquer les Exigences thématiques conformément aux Normes internationales d'audit interne. La conformité aux Exigences thématiques est obligatoire pour les activités d'assurance et recommandée pour les activités de conseil.

L'Exigence thématique est applicable lorsque le thème est l'un des suivants :

1. Le thème d'une mission figure dans le plan d'audit interne.
2. Le thème a été identifié lors de la réalisation d'une mission.
3. Le thème d'une mission demandée ne figure pas dans le plan d'audit interne initial.

L'applicabilité de chaque exigence de l'Exigence thématique doit être évaluée. Les éléments probants de ces évaluations doivent être documentés et conservés. Toutes les exigences peuvent ne pas s'appliquer une à une à chaque mission ; si certaines d'entre elles sont exclues, une justification doit être consignée et conservée. La conformité à l'Exigence thématique est obligatoire et sera évaluée lors des évaluations de la qualité.

Pour plus d'informations, voir le Guide de l'utilisateur de l'Exigence thématique relative à la résilience organisationnelle.

Résilience organisationnelle

La résilience organisationnelle est définie comme la "capacité d'une organisation à absorber et à s'adapter à un environnement changeant" dans la norme ISO 22316:2017, Sécurité et résilience - Résilience organisationnelle - Principes et attributs, publiée par l'Organisation internationale de normalisation. La résilience organisationnelle

est un vaste sujet qui couvre d'importants éléments stratégiques, opérationnels, technologiques, humains, sociaux et financiers. La résilience organisationnelle concerne les risques susceptibles de perturber ou de porter atteinte de manière significative à la capacité d'une organisation à fournir ses produits et services clés, à préserver la confiance des parties prenantes ou à atteindre ses objectifs stratégiques. Ces risques peuvent résulter d'événements soudains (tels que des catastrophes naturelles, des cyberattaques et des conflits géopolitiques), de pressions environnementales prolongées (telles que la raréfaction des ressources et les crises de santé publique) ou de changements dans l'environnement (tels que des disruptions technologiques, des changements réglementaires et l'érosion de la réputation). Ces risques peuvent également être des changements graduels ou des pressions progressives qui, au fil du temps, compromettent la stabilité et la capacité d'adaptation d'une organisation. Les risques de ce type survenant progressivement peuvent être parfois négligés. Les organisations résilientes anticipent les risques à la fois soudains et progressifs et s'y adaptent pour réussir.

Les facteurs de risque inhérents qui augmentent la menace sur la résilience comprennent une grande complexité opérationnelle, des chaînes d'approvisionnement globalisées, une infrastructure ou des systèmes de données centralisés, une disponibilité limitée de la main-d'œuvre, des conditions de marché volatiles et une forte dépendance à l'égard de tiers ou de zones géographiques critiques. Les organisations exerçant dans des secteurs requérant une haute fiabilité ou soumis à des contrôles réglementaires étroits peuvent également être confrontées à des risques par nature plus élevés en raison de leurs impacts sur le public et des obligations de conformité.

Les auditeurs internes évaluent généralement les processus et les contrôles des technologies de l'information (TI) relatifs à la continuité des activités et à la reprise après sinistre. Un plan de continuité des activités détaille les étapes à suivre par une organisation pour revenir à un fonctionnement opérationnel normal en cas de sinistre. Un plan de reprise après sinistre décrit comment les organisations protégeront leurs systèmes informatiques et leurs données critiques en cas d'interruption d'activité. La résilience organisationnelle nécessite également une planification stratégique, une gestion des risques d'entreprise, un leadership et une culture efficaces, ainsi que des processus de contrôle à l'échelle de l'organisation. Disposer de processus de contrôle solides en termes de résilience organisationnelle permet non seulement aux organisations d'anticiper, de se préparer, de réagir et de s'adapter en permanence au changement, mais aussi de survivre et de se développer.

Évaluer la résilience organisationnelle des processus de gouvernance, de gestion des risques et de contrôle

Cette Exigence thématique fournit une approche cohérente et complète de l'évaluation de la conception et de la mise en œuvre des processus de gouvernance, de gestion des risques et de contrôle de la résilience organisationnelle. Les exigences représentent une base a minima pour l'évaluation de la résilience organisationnelle.

Gouvernance

Exigences :

Les auditeurs internes doivent évaluer les aspects suivants de la gouvernance de la résilience organisationnelle :

A. Une stratégie formelle de résilience organisationnelle est établie et documentée par le Conseil, avec des objectifs qui s'alignent sur la mission et la vision de l'organisation et les soutiennent. La stratégie porte

sur les éléments opérationnels, technologiques et financiers nécessaires pour se défendre et poursuivre les opérations en cas de crises, de perturbations et de situations d'urgence, et sur la manière de se rétablir et de s'adapter par la suite. La stratégie s'aligne sur l'approche d'ensemble de l'organisation en matière de gestion des risques et est testée et mise à jour périodiquement.

B. Des informations à jour quant à la réalisation de la stratégie et des objectifs de résilience de l'organisation sont périodiquement communiquées au Conseil pour examen. La surveillance stratégique, les processus de planification à long terme et la culture de l'organisation intègrent sa capacité de résilience. Elle est notamment prise en compte dans les ressources et les budgets nécessaires aux activités commerciales et opérationnelles clés.

C. Les processus opérationnels, technologiques et financiers critiques liés à la résilience organisationnelle ont été identifiés. Des politiques et des procédures ont été établies pour ces processus critiques ; elles sont examinées périodiquement et mises à jour si nécessaire pour renforcer l'environnement de contrôle.

D. Une structure de commandement destinée à la prise en charge des incidents est mise en place, elle comprend des hiérarchies décisionnelles, des protocoles de communication et d'escalade, ainsi que des rôles et responsabilités au niveau opérationnel et au niveau de la direction. Cette structure est utilisée pour surveiller et contribuer à l'établissement d'objectifs de résilience organisationnelle.

E. Un processus est mis en place pour réévaluer périodiquement les compétences des personnes jouant un rôle essentiel dans les processus de résilience. Il existe un plan de succession qui identifie les postes clés et les candidats potentiels à un éventuel remplacement.

F. Un processus est mis en place pour impliquer les parties prenantes internes et externes concernées par l'identification, l'analyse et les réponses à apporter aux vulnérabilités existantes et aux menaces émergentes susceptibles d'affecter la réalisation des objectifs de résilience de l'organisation. Les parties prenantes peuvent inclure la direction générale, les opérationnels, les acteurs de la gestion des risques, de l'informatique, de la chaîne d'approvisionnement/achats, de la gestion des établissements, des ressources humaines, de la finance, du service juridique, de la conformité, des relations publiques, les fournisseurs importants, les clients, les autorités de réglementation, etc.

GESTION DES RISQUES

Exigences :

Les auditeurs internes doivent évaluer les aspects suivants de la gestion des risques liés à la résilience de l'organisation :

A. Les processus d'évaluation et de gestion des risques de l'organisation comprennent l'identification, l'analyse, l'atténuation et le suivi des menaces susceptibles de perturber les opérations. La stratégie de gestion des risques liés à la résilience de l'organisation est communiquée à l'ensemble de l'organisation et examinée périodiquement.

B. Les risques liés à la résilience de l'organisation sont périodiquement évalués et gérés dans l'ensemble de l'organisation. L'évaluation et la gestion des risques peuvent porter sur les domaines suivants : opérations, gestion des risques d'entreprise, informatique, chaîne d'approvisionnement/achats, établissements, ressources humaines, finances, juridique, conformité, réglementation, relations publiques, fournisseurs critiques, réputation, risques émergents, etc.

C. L'obligation de rendre compte et la responsabilité de la gestion des risques liés à la résilience de l'organisation sont établies. Une personne ou une équipe est désignée pour suivre et rendre compte périodiquement de la manière dont les risques liés à la résilience organisationnelle sont gérés, notamment les ressources nécessaires pour atténuer les risques et identifier les menaces émergentes portant sur la résilience organisationnelle.

D. Un processus est en place pour suivre les niveaux de risques liés à la résilience de l'organisation (émergents ou déjà identifiés) et escalader rapidement ceux qui atteignent un niveau considéré comme inacceptable, au regard des lignes directrices de gestion des risques et de la tolérance au risque de l'organisation, ou des exigences légales et réglementaires applicables. Les impacts financiers et non-financiers des risques liés à la résilience organisationnelle sont pris en compte.

E. La direction a mis en place et teste périodiquement les processus de réponse et de reprise en cas de crises, perturbations ou situations d'urgence. Le processus de réponse aux incidents et de reprise comprend la détection, l'endiguement, la restauration et l'analyse post-incident. L'approche de réponse aux incidents comprend des analyses de scénarios et des tests périodiques de résistance à une liste d'événements perturbateurs plausibles. Les résultats de ces exercices sont examinés par le Conseil et la direction générale, et les mesures d'amélioration sont suivies et communiquées périodiquement. Les recommandations sont applicables. La responsabilité de leur mise en œuvre est clairement définie et les délais de mise en œuvre sont fixés.

CONTRÔLES

Exigences :

Les auditeurs internes doivent évaluer les aspects suivants des processus de contrôle liés à la résilience de l'organisation.

A. Un processus est mis en place pour identifier les fournisseurs et tiers critiques (fournisseurs et prestataires) et les niveaux de stocks minimums nécessaires à la poursuite des opérations vitales. Ce processus comprend la mise à jour d'une liste de fournisseurs alternatifs.

B. Les données critiques pour les opérations sont identifiées et classifiées. La classification des données comprend leur localisation de stockage, l'identification des personnes qui doivent y avoir accès, les modalités de leur accès et leur inclusion ou non au périmètre de sauvegarde et leurs modalités de restauration en cas d'urgence.

C. Des contrôles IT essentiels et un suivi en continu sont en place pour réduire les risques liés à la sécurité de l'information (y compris les risques cyber) et garantir la protection des données sensibles en cas de crise, de perturbation ou d'urgence. Les contrôles et le suivi continu comprennent la veille en temps réel sur les menaces et les restrictions d'accès aux seuls utilisateurs autorisés.

D. Les actifs informatiques critiques sont inventoriés. Ces actifs comprennent notamment les matériels, les logiciels et les services nécessaires au soutien des opérations lors de crises, de perturbations et d'urgences.

E. Des plans de continuité des activités et de reprise après sinistre sont établis. Ces plans comprennent des rôles attribués au personnel affecté et aux équipes en charge de la reprise. Ces plans sont testés périodiquement (par exemple, un "exercice sur table") et les résultats des tests, y compris les possibilités d'amélioration, sont communiqués au Conseil et à la direction générale.

F. Un processus est en place pour adapter l'environnement de travail en cas de crise, de perturbation ou d'urgence. Ces adaptations peuvent inclure l'utilisation d'autres lieux de travail, comme le travail à domicile ou l'installation d'un bureau temporaire en temps opportun et de manière efficace.

G. Un processus est mis en place pour suivre en continu et signaler les menaces émergentes et les vulnérabilités liées à la résilience de l'organisation et pour recenser, hiérarchiser et mettre en œuvre les opportunités d'amélioration des opérations de résilience de l'organisation. Ce processus peut inclure des systèmes d'alerte ou de veille et collecte de renseignements sur les risques.

H. Un processus est mis en place pour sensibiliser et former le personnel à la résilience de l'organisation, en veillant à ce qu'il connaisse les politiques et les procédures à suivre et les mesures à prendre en cas de crise, de perturbation ou d'urgence. Le processus comprend des exercices d'entrainement au cours desquels des scénarios de perturbations sont simulés.

I. Un processus est mis en place pour s'assurer que les ressources humaines, technologiques et financières nécessaires sont inscrites au budget et disponibles en cas de crise, de perturbations ou d'urgence. Ce processus peut inclure un financement approuvé a priori.

J. Les ressources financières nécessaires au soutien de la résilience de l'organisation sont périodiquement analysées et communiquées au Conseil. Cette analyse comprend l'évaluation des liquidités, de la couverture par les assurances et des dispositifs de financement d'urgence.

K. Un processus est en place pour examiner les crises, les perturbations et les situations d'urgence après leur survenance et pour analyser les revues post-incidents dans le cadre d'un processus d'apprentissage, y compris l'intégration des enseignements tirés de l'expérience dans la planification future de la résilience de l'organisation.

À propos de l'Institut des auditeurs internes

L'IIA est une association professionnelle internationale qui compte plus de 265 000 membres dans le monde et a délivré plus de 200 000 certifications Certified Internal Auditor® (CIA®) dans le monde entier. Fondée en 1941, l'IIA est reconnue dans le monde entier comme le leader de la profession d'audit interne en matière de normes, de certifications, d'éducation, de recherche et de conseils techniques. Pour plus d'informations, consultez le site www.theiia.org.

Droit d'auteur

Septembre 2025

